tioners now attribute the majority of
ılting from human error. According to
ulnerability and configuration manage-
ualized."[12] Also according to Gartner,
security vulnerabilities will be intro-
ismanagement.[13] Why is this the case,
rtual server images can be replicated far
ed, require great effort to discover and
Analysts have published some startling
ty implications: Gartner predicts that
ion VMs will be less secure than their
ercent of deployments [will be associ-
."[15]

ave to be this way. If the principles of
to be valid in any technology domain,
an inherently unsecure new technology
e next as yet unforeseen major technol-
information security is seen as a key
IT services, confidentiality, integrity,

st Practices for Securing Virtual Machines," by

irtualization" by Neil MacDonald, November

4

Information Classification

Jennifer Bayuk

Information classification, related to information security, is concerned with placing information into categories related to how securely it should be handled with respect to access control and confidentiality protection. This section deals with the issues associated with classifying information with respect to its security handling. First is the issue of who is qualified to make this determination. The next issue deals with the sense that this decision is often context and content dependent, and can change with time and circumstances. For example, a seemingly innocuous piece of information may not seem very revealing, but taken in combination with other information may become much more sensitive. For example there are many women who may be characterized as blonde and 5-feet tall. Linking some financial information to the fact that the person is a blonde female who is 5-feet tall may not be very revealing, but if I add that the woman lives on Montgomery Sreet in Cleveland, Ohio, we may have reduced the possibilities down to a single individual. So the context within which a piece of information is known can be very important and change the sensitivity of the information. The content is also important. It may not be terribly important to know that John Smith has a $100 dollars in his checking account, but if it were known that John Smith has over $100,000 in his checking account, we might decide that this information is extremely sensitive. Over time, as new types of attacks and fraudulent patterns appear, we might change our minds about the sensitivity of a piece of information; for example phishing has made it much more sensitive to know the email address or phone number of a customer of your bank than it was some 10 years ago. So, classification systems should be dynamically changing in terms of context, content, and

past history. The determination of the correct classification of an item of information might well involve the input of business and security professionals as well as data provided by data center resource managers.

—D.S.

4.1 Background

Information classification is the act of labeling information. A label on a piece of information enables it to be treated as an object. It may be reasoned about without concentration on its composition. It enables different information with the same label to be treated as a set, as one object. In the field of information security, information labeling is a prerequisite for providing appropriate *handling procedures*. Information handling procedures are instructions on how to deal with information when it is stored as data in computers or as text on printed materials. The basic process is depicted in Figure 4.1.

A common and well-understood example of information classification comes from the military. Military information labels include: *top secret, secret,* and *unclassified*. Before information was stored in computers, it was stored in documents, file cabinets, and locked rooms that were stamped with these labels. For several decades in the early days of computers, the military classification was the basis of general study into how to secure data in a computing environment, and also the basis of specific algorithms used to secure operating system files.

The military information classification approach was hierarchical. *Top secret* was a higher level classification than *secret*, *unclassified* was lower than *secret*. When applied to sets of information on computers, the hierarchical labeling system presented issues to be addressed. For example: how to prevent people who should only have access to *unclassified* data from having access to *secret* data while still allowing those with *secret* access to have *unclassified* data on the same computer. In an attempt to resolve such issues, labels were assigned to sets of people as well as the data. The same labels were used and a person was assumed to be on the same level in the hierarchy as the data they accessed. A *secret* person could read *secret* and *unclassified* data while a *top secret* person could read *top secret*, *secret* and *unclassified* data. Any information produced by a *top secret*

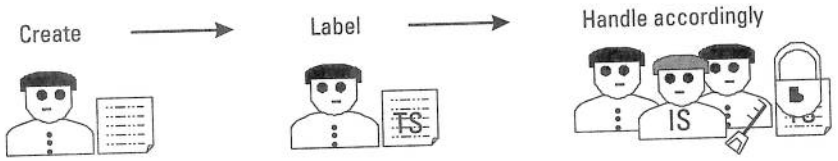


Figure 4.1 Information classification activity.

person was assumed by the compu
person would be able to read it.

Implementation issues with
any *unclassified* person produced
a computer, the individual could
edit after having written it. This
standards, where individual file
are commonplace, but unless o
cleared at the *top secret* level, it
sounds.

Though the military was th
of data to receive special handlin
soon caught up. Confidentiality
tion schemes to be applied to no
lysts tried to map confidentiality
schemes designed for military
classification models.

For example, a typical orgar
for information, following a hiera

- Public;
- Proprietary;
- Proprietary Restricted.

At such an organization, pr
each classification level. Often c
would be designed to keep data
lower level. Illustrated in Figure
sistent protection profile aroun
ments for information security.

For example, all documen
stamped with one of the three l
ment itself. The protection profil

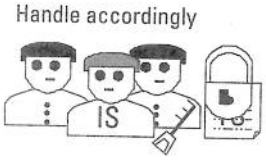
Information classification and labeling

Figure 4.2 Information classification

ect classification of an item of
f business and security profes-
r resource managers.

—D.S.

information. A label on a piece of
t. It may be reasoned about with-
es different information with the
In the field of information secu-
providing appropriate *handling*
are instructions on how to deal
computers or as text on printed
re 4.1.
ple of information classification
labels include: *top secret, secret,*
d in computers, it was stored in
t were stamped with these labels.
ers, the military classification was
ata in a computing environment,
secure operating system files.
approach was hierarchical. *Top*
cret, unclassified was lower than
computers, the hierarchical label-
example: how to prevent people
from having access to *secret* data
ave *unclassified* data on the same
s, labels were assigned to sets of
used and a person was assumed
ata they accessed. A *secret* person
top secret person could read *top*
ation produced by a *top secret*



person was assumed by the computer to be labeled *top secret* and no *unclassified* person would be able to read it.

Implementation issues with the hierarchy quickly arose. For example: if any *unclassified* person produced data that was subsequently labeled *secret* using a computer, the individual could no longer read it, nor even to have a copy to edit after having written it. This seems a simple problem to solve by today's standards, where individual file object ownership and role-based entitlements are commonplace, but unless one can assume system administrators are all cleared at the *top secret* level, it is still not as technically easy to resolve as it sounds.

Though the military was the first to recognize the value of creating classes of data to receive special handling, privacy and intellectual property advocates soon caught up. Confidentiality in computing required information classification schemes to be applied to nonmilitary scenarios. Information security analysts tried to map confidentiality requirements onto information classifications schemes designed for military use. They devised similar hierarchical data classification models.

For example, a typical organization may have between three and five labels for information, following a hierarchy such as:

- Public;
- Proprietary;
- Proprietary Restricted.

At such an organization, procedures would be created for handling data at each classification level. Often called a *protection profile*, this set of procedures would be designed to keep data at a higher level more secure than data on a lower level. Illustrated in Figure 4.2, the assumption is that maintaining a consistent protection profile around information of a given class meets requirements for information security.

For example, all documents in the organization may be required to be stamped with one of the three labels or have the label embedded in the document itself. The protection profiles may allow *public* documents to be left about,

Figure 4.2 Information classification assumption.

whereas *proprietary* documents may be shared only with employees, and documents labeled *proprietary restricted* may be shared only with those who have a need to know and are not to be left unattended. Procedures designed to keep *proprietary* and *proprietary restricted* information confidential may include desktop audits wherein any unattended desktop that has information labeled *proprietary restricted* fails audit. Metrics might be kept by department and departments required to be 100% compliant.

4.2 Observations

Organizations that use this type of hierarchical classification scheme typically have a common struggle in achieving confidentiality goals. It is often the case that guidelines for determining what information should be stamped with which label are not straightforward and thus not easily understood. Inaccurate judgment on whether information is *proprietary* or not leads to mislabeling. Mislabeling leads to mishandling. The fatal flaw in most conventional information classification programs is that they lack procedures for the *labeler*.

Where information classification is focused on the end result of the labeling process—information handling, the *labeler* is left without any guidance. This focus is so prevalent that it is common in information security literature to see information classified with words that specify the handling criteria, as opposed to any attribute of the information itself. For example, here is a common textbook description of information classification labels:[1]

1. Information that does not need safeguarding;
2. Information that must be safeguarded against loss or threats to integrity;
3. Information that, if disclosed to unauthorized parties, could result in reputation or financial damage;
4. Information that, if changed by or disclosed to unauthorized parties, could result in threats to an organization's existence.

From these labels, information-handling procedures are trivial to derive, for example:

A. No need to protect;
B. Need to prevent write-access by unauthorized individuals;

1. To avoid direct criticism of any specific textbook which may contain otherwise sound information security education, I will omit reference to any one volume.

C. Need to prevent read-acce
D. Need to control and trac and write–access.

Textbooks advocate that proc dle information (e.g., the clear desk extremely simple to follow. Once must be safeguarded against loss security classification program wil *individuals* be configured in every s and methods to ensure that acces that *authorized* group. There woul group members whereby docur changes to membership. It would member of the *authorized* group) information classification in orde configuration in itself would be d requirements.

Where information security trols within the systems environm ing the labeling function (the *la* success of any information classif ever, is left to the end user. Infor that, where the derivation of han tion of the information itself, the order for *the labeler to perform th* content of the data, and be cogi These include not only threats t resulting from unmet regulatory r the data in the custody of the en its content to perform analysis to by itself or in combination wi informed judgment, justify the a to 3), depending how many level

The activity described abo *labeling*, is the core of any infor tinue to present the last step, the D are appropriate requirements sional practice with respect to i sentation of information classifi do information analysis makes it derive information-handling pr

only with employees, and docu-
ıred only with those who have a
ed. Procedures designed to keep
n confidential may include desk-
ıt has information labeled *propri-*
t by department and departments

al classification scheme typically
ntiality goals. It is often the case
ıation should be stamped with
ıot easily understood. Inaccurate
ary or not leads to mislabeling.
w in most conventional informa-
ɔcedures for the *labeler.*
ed on the end result of the label-
er is left without any guidance.
information security literature to
ıpecify the handling criteria, as
self. For example, here is a com-
fication labels:[1]

ıarding;
:ded against loss or threats to

uthorized parties, could result in

lisclosed to unauthorized parties,
ion's existence.

; procedures are trivial to derive,

thorized individuals;

ıich may contain otherwise sound infor-
y one volume.

C. Need to prevent read-access by unauthorized individuals;
D. Need to control and trace accountability for each instance of read- and write–access.

Textbooks advocate that procedures subsequently developed to safely handle information (e.g., the clear desk and nightly audits) should be designed to be extremely simple to follow. Once information is classified as information that must be safeguarded against loss or threats to integrity, an ideal infomation security classification program will have provisions that a group of *authorized individuals* be configured in every system that contains information of that type, and methods to ensure that access to data of that type is restricted to users in that *authorized* group. There would be an auditable authorization process to add group members whereby documentation trails provide accountability for changes to membership. It would be assumed that the actual data handler (i.e., member of the *authorized* group) need not know much if anything about the information classification in order to correctly protect it. Rather, the system configuration in itself would be designed to enforce the information protection requirements.

Where information security professionals are totally occupied with controls within the systems environment, the assumption that the person performing the labeling function (the *labeler*) is qualified to do so, is critical to the success of any information classification program. The labeling function, however, is left to the end user. Information security curriculums overlook the fact that, where the derivation of handling procedures is automatic from the definition of the information itself, the labeling process itself is extremely difficult. In order for *the labeler to perform the labeling*, he or she must first understand the content of the data, and be cognizant of the risk of data exposure to threats. These include not only threats to the enterprise data owner, but consequences resulting from unmet regulatory requirements. The person would have to survey the data in the custody of the enterprise and utilize his or her understanding of its content to perform analysis to identify the distinct types of data which either by itself or in combination with data of other types, would, in his or her informed judgment, justify the assignment of one the labels (1 to 4, 1 to 5, or 1 to 3), depending how many levels an organization has chosen to adopt.

The activity described above, as that required for *the labeler to perform the labeling*, is the core of any information classification effort. Yet textbooks continue to present the last step, the analysis which leads to the conclusion that A to D are appropriate requirements given 1 to 4, as the infomation security professional practice with respect to information classification. The elementary presentation of information classification levels prior to the instruction on how to do information analysis makes it easy for an information security professional to derive information-handling procedures and masks the true complexity of the

analysis leading up to the label. The omission of the actual core classification process often creates a disconnect between those who understand the content of the data and the infomation security professional assigned to protect it.

This type of classification process seems to have its roots in information security risk analysis efforts that focus on disclosure consequences. A typical risk analysis is concerned with the impact to the organization from potential harm to confidentiality, integrity, and availability of data. Such analysis also assumes that there is an omniscient business person, like the data labeler, who can make the decisions on how the business would be affected by confidentiality, integrity, and availability lapses with no guidance. Like the textbook information classification process, the textbook risk analysis process assumes that the information security professional is handed the outcome of the business decision and need only develop corresponding handling procedures.

The leap from disclosure consequences to handling mechanisms suffers from a fundamental omission, one that often leaves decisions concerning actual information classification out of the information security curriculum. The fact that the decision on how to label information is outside the realm of the information security curriculum takes the information protection responsibility away from the realm of the security professional and leaves it in the hands of the end user. End users are usually given guidelines such as 1 to 4 above and asked to classify their data. In any organization where multiple individuals may have control of similar and very specific fields of information, and also more than one data storage area, this could easily result in the inconsistent application of controls.

To make it easy on themselves, information security professionals facing choices in data handling procedures often fall back to the principle of least privilege. That is, all individuals should only have the minimum privileges to read or write data to the extent these are absolutely necessary to continue the smooth operation of the organization. It then becomes a question of how hard the InfoSec controls make it for a person who is not authorized to see the data and to actually get to it. It is also a question of where the controls are placed. Application users, for example, have got to be able to view the data in the clear (i.e., not encrypted). Database administrators do not have to actually view it, but have to have access to view it in order to troubleshoot the jobs that retrieve and load it. Job control professionals need to actually run the jobs (so by transitive trust have access to any encryption keys that are used by those jobs).

Note that the principle of least privilege itself is subject to interpretation. One organization will argue with clear conscience that job control administrators need access to data to troubleshoot jobs, while another organization will insist that no administrators should have access on a day-to-day basis, but that access to troubleshoot should only be granted at the point jobs fail. This continuum between easy access to support operations and absolute minimum need to know creates an economic argument for detective security measures rather than

preventive. Where access c
upon potentially unauthoriz
by reference to operational s

Despite the wide vari
handling procedures, inforı
determine whether inform
operations job responsibiliti
trate on whether the inforı
whether risks are reported t
on appropriate policies and
has access to what type data
age IT control professional.

The result is that info
have not been focused on s
have been caught up with
approaches to information s
sion have resulted in inform

- Aggregated data an
- Enterprise-wide pr
- Weighing threat an

This thousand-foot
ignores actual data content.
executive management refle
grams have been using hie
approaches pass "internal c
for enterprise-wide change.
efforts and handling require
of application developers m
of data.

4.3 Recommendations

The information security in
the advent of the payment
credit card data (PCI DSS),
sification has entered the rea

2. Payment Card Industry Data

ission of the actual core classification
1 those who understand the content of
ssional assigned to protect it.
eems to have its roots in information
disclosure consequences. A typical risk
e organization from potential harm to
f data. Such analysis also assumes that
e the data labeler, who can make the
affected by confidentiality, integrity,
ike the textbook information classifi-
process assumes that the information
ne of the business decision and need
edures.
ices to handling mechanisms suffers
en leaves decisions concerning actual
nation security curriculum. The fact
n is outside the realm of the informa-
ation protection responsibility away
and leaves it in the hands of the end
uch as 1 to 4 above and asked to clas-
ultiple individuals may have control
iation, and also more than one data
consistent application of controls.
mation security professionals facing
ll back to the principle of least privi-
e the minimum privileges to read or
y necessary to continue the smooth
omes a question of how hard the
s not authorized to see the data and
here the controls are placed. Appli-
le to view the data in the clear (i.e.,
not have to actually view it, but
ubleshoot the jobs that retrieve and
tually run the jobs (so by transitive
are used by those jobs).
ge itself is subject to interpretation.
cience that job control administra-
s, while another organization will
ess on a day-to-day basis, but that
l at the point jobs fail. This contin-
ns and absolute minimum need to
ctive security measures rather than

preventive. Where access controls are left flexible, but alerts may be devised upon potentially unauthorized data access, the unexpected access can be justified by reference to operational situations.

Despite the wide variety of choices in implementing least-privilege data handling procedures, information security professionals and auditors routinely determine whether information is appropriately handled without giving IT operations job responsibilities more than a cursory glance. They instead concentrate on whether the information security program is appropriately managed, whether risks are reported to upper management, and whether documentation on appropriate policies and procedures exist. Actual verification of who really has access to what type data is way beyond the expertise of even the above average IT control professional.

The result is that information security literature and educational materials have not been focused on securing specific classes of information, but instead have been caught up with organizational risk reduction measures. Historical approaches to information classification within the information security profession have resulted in information-handling countermeasures focused on:

- Aggregated data and infrastructure securing them;
- Enterprise-wide processes rather than data protection goals;
- Weighing threat and vulnerabilities against business acceptance of risk.

This thousand-foot view of information handling almost completely ignores actual data content. Within such organizations, there has not been much executive management reflection on the fact that enterprise-scale security programs have been using hierarchical approaches to data classification. Where approaches pass "internal control" audits year after year, there is not much call for enterprise-wide change. So the burden for actual information classification efforts and handling requirements, where they exist, have fallen into the hands of application developers meeting specific business requirements for a given set of data.

4.3 Recommendations

The information security information classification landscape is changing. With the advent of the payment card industry's data security standards for securing credit card data (PCI DSS), the real analysis required by proper information classification has entered the realm of the information security literature.[2] Figure 4.3

2. Payment Card Industry Data Security Standard, PCI DSS Version 1.1.

Applicable if a Primary Account Number (PAN) is stored, processed, or transmitted.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN.
**Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

Figure 4.3 Excerpt from PCI Data Security Standards, Version 1.1.

indicates the prescriptive nature of PCI DSS requirements with respect to labeling certain fields of data as *protection required*. It indicates, for example, that certain data fields may be unprotected in isolation, but are considered *protection required* when stored in conjunction with other fields. These are labeling requirements at the semantic level. They require assignment of labels to information as opposed to data.

Information that is properly labeled allows the handling requirements to be specified as network, operating system, and application security requirements surrounding the end-to-end transmission and storage of data within the organization. In the case of PCI DSS, these requirements are quite specific:[3]

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for security parameters.
3. Protect stored cardholder data (see detail with respect to PAN).
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.

3. Ibid.

7. Restrict access to cardhold
8. Assign a unique ID to each
9. Restrict physical access to
10. Track and monitor all a data.
11. Regularly test security syst
12. Maintain a policy that adc

Further detail in the standard tion with the definitions in Figure *unencrypted* in isolation, but must b other fields. The information label handling procedure *encryption*.

Though privacy laws and mum-security requirements existed requirements for businesses to take these requirements have for some tin partners in the form of legal contra requirements, such as industry assc organizations, also influence any inc exercises (see Figure 4.4). It is not u to be compliant with a myriad of re ing begun a true internal informatio

It took the low-level technica lated with the level of analysis requi map it to associated information-h tion-handling procedures are direct mation data fields themselves, no m they sit in the organization's infrast nition for data fields, pursued at an choices more obvious. Infosec prof that originate in industry consens requirements are clearly mapped to uating technical alternatives, and t goals, notably that of protecting pri

4. For example, GLBA and EU Data Priva

nd Privacy

stored,

Storage ermitted	Protection Required	PCI DSS Req. 3.4
YES	YES	YES
YES	YES*	NO
YES	YES*	NO
YES	YES*	NO
NO	N/A	N/A
NO	N/A	N/A
NO	N/A	N/A

n conjunction with the PAN.
subsequent to

sion 1.1.

irements with respect to label-
ıdicates, for example, that cer-
but are considered *protection*
lds. These are labeling require-
ent of labels to information as

the handling requirements to
lication security requirements
age of data within the organi-
s are quite specific:[3]

ıration to protect cardholder

security parameters.
with respect to PAN).
across open, public networks.
ıre.
l applications.

7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Further detail in the standard reveals that requirement three, in conjunction with the definitions in Figure 4.3, means that certain data fields may be *unencrypted* in isolation, but must be *encrypted* when stored in conjunction with other fields. The information label *protection required* is supplemented with the handling procedure *encryption*.

Though privacy laws and similar field-specific counterparty minimum-security requirements existed before PCI DSS,[4] they were not perceived as requirements for businesses to take detailed technical measures. Nevertheless, these requirements have for some time been coming from customers and business partners in the form of legal contracts and service agreements. Other sources of requirements, such as industry associations and independent standards setting organizations, also influence any individual company's information classification exercises (see Figure 4.4). It is not uncommon to see InfoSec professionals claim to be compliant with a myriad of regulations and requirements without ever having begun a true internal information classification effort.

It took the low-level technical detail of PCI DSS to confront those regulated with the level of analysis required to perform information classification and map it to associated information-handling procedures. In this model, information-handling procedures are directly derived from the definition of the information data fields themselves, no matter what the end user labels them or where they sit in the organization's infrastructure. In this model, a clear semantic definition for data fields, pursued at an industry level, makes information protection choices more obvious. Infosec professionals should embrace labeling processes that originate in industry consensus on data modeling. Because the handling requirements are clearly mapped to the data label, there are clear criteria for evaluating technical alternatives, and thus clear measures for success in achieving goals, notably that of protecting privacy.

4. For example, GLBA and EU Data Privacy Laws.

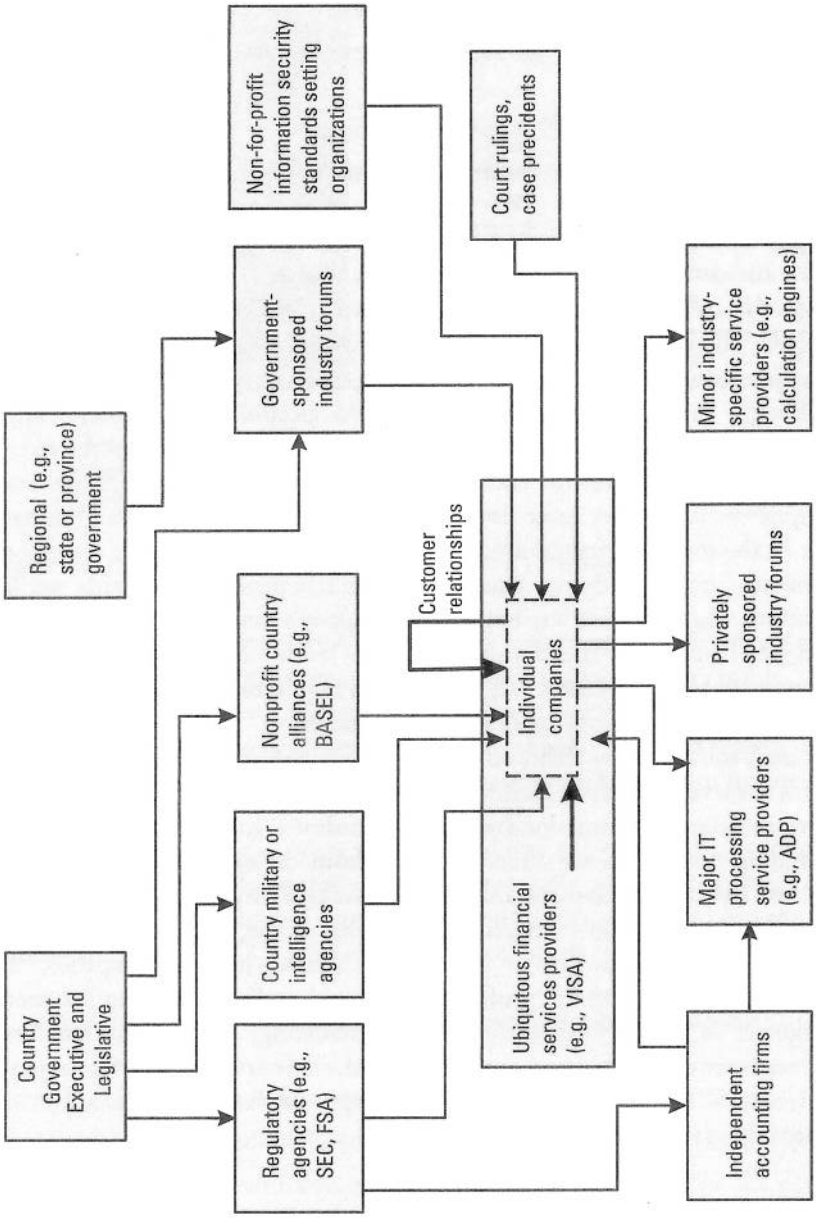


Figure 4.4 Requirements sources.

4.4 Future Trends

The technical expectations that
information classification exercis
archical set of labels and place s
ture. For an information secu
practice, information security
modeling. Control points of the
architectural wheels. The archit
ponents it does today, but it will

At the core of any informa
Where data are stored electroni
people are familiar with files an
technical environments, it is m
els, that is, to identify interdepe
of object in the enterprise envir
wherein data are either compl
relationships, or via links that a
vidual object as part of its own
cal implementation that takes a
depicted in the model.

Figure 4.5 shows the sam
in a few different ways. It also il
procedures may be developed a
on the data structure in which t
information in the hierarchical
the relational model at the tab
level.

In all models, it may be p
linked only to descriptions or b
tomer to whom the account be
gies such as encryption and dat
when applied to certain fields a
in another. As information clas
ated handling procedures mor
professional will by necessity b
and technical implementatio
meets requirements will no lon
profiles, but also involve archit
ration strategies, and source co

5. Note that these are three widely u

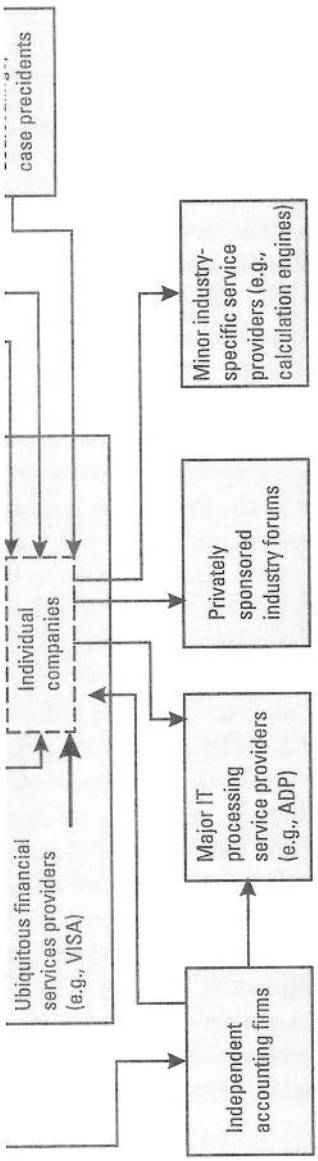


Figure 4.4 Requirements sources.

4.4 Future Trends

The technical expectations that accompany the PCI DSS have set a new bar for information classification exercises. It is no longer best practice to assume a hierarchical set of labels and place similar labels on information storage infrastructure. For an information security organization to embark on the new best practice, information security professionals must become cognizant of data modeling. Control points of the future will be cogs on very large enterprise-wide architectural wheels. The architecture will include the same infrastructure components it does today, but it will have an overlay of a data model.

At the core of any information handling process is an information model. Where data are stored electronically, they may be divided in many ways. Most people are familiar with files and directories in hierarchical structures. In highly technical environments, it is more common to think of data in relational models, that is, to identify interdependencies among data concerning different types of object in the enterprise environment. There are also object-oriented models, wherein data are either completely encapsulated by hierarchical parent-child relationships, or via links that allow multiple objects to include the same individual object as part of its own definition.[5] Each model will have its own technical implementation that takes advantage of the relationships between the data as depicted in the model.

Figure 4.5 shows the same basic set of data on customer accounts stored in a few different ways. It also illustrates that the ways in which permissions and procedures may be developed around information handling will often depend on the data structure in which the information is stored. For example, customer information in the hierarchical model may be protected at the folder level, in the relational model at the table level, and in the object model, at the object level.

In all models, it may be possible to expose account information when it is linked only to descriptions or balances without disclosing the name of the customer to whom the account belongs. However, information security technologies such as encryption and data masking may have serious performance impacts when applied to certain fields accessed via one technical implementation and less in another. As information classification becomes more field-driven and associated handling procedures more proscriptive, the average information security professional will by necessity be more and more involved in data architecture and technical implementation strategies. Verification that implementation meets requirements will no longer be a matter of maintaining generic protection profiles, but also involve architecture and design review, infrastructure configuration strategies, and source code vulnerability testing. As discussed above, this is

5. Note that these are three widely used models, but there many other ways of depicting data.

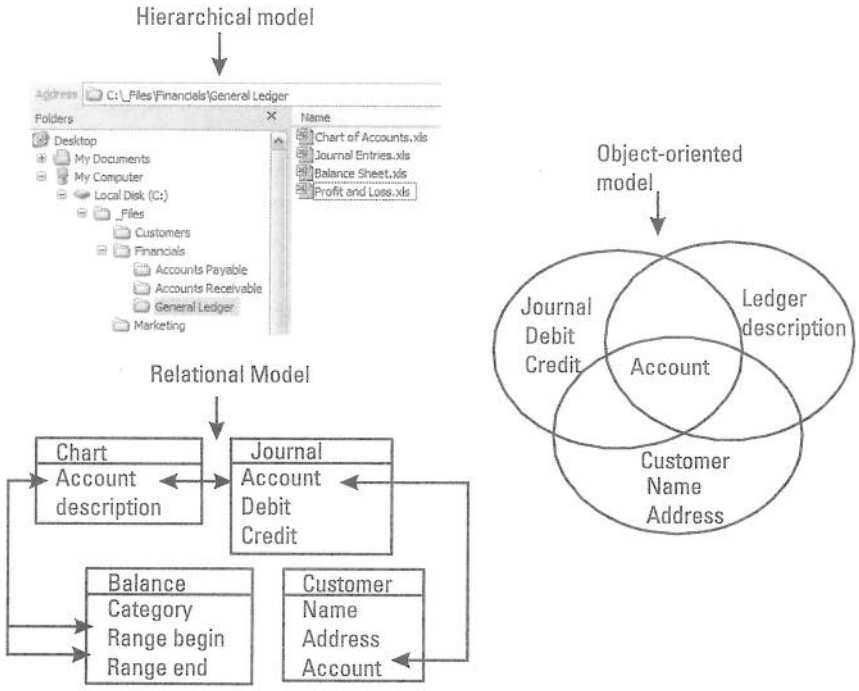


Figure 4.5 Data models.

already being done by application development teams as specific technical protection requirements become more prevalent. Economies of scale dictate that this activity be elevated to the level of the organizational information security program.

5

Human Factors

Mahi Dontamsetti

Security deals with the protectic
maintaining confidentiality (prev
integrity of the source and conte
ing), and providing access contr
and authorized). Privacy deals v
access to, whom you share it wi
protection also involves providin
information you are using. In th
serve as a tool to help ensure priva
such as when you monitor em
observe and stop fraudulent beh
there is often a delicate balancing
monitoring for fraudulent behav
concern for privacy is generally re
privacy violation, such as inciden
incidents of identity theft and re
privacy of sensitive customer fina
lation in this area. Other sensit
secrets and intellectual property. I
rity and the general difficulty in
was largely in paper form, and st
Today with increasingly large